NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 1600.1
Effective Date:
November 03, 2004
Expiration Date:
November 03, 2014

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA Security Program Procedural Requirements w/Change 2 (4/01/2009)

Responsible Office: Office of Protective Services

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | AppendixJ | AppendixK | AppendixL | AppendixM | AppendixN | AppendixO | ALL |

Chapter 4: NASA Personnel Security Program: Risk Designation Process, Background Investigations, and Access Determinations for NASA Contractor Employees

4.1 General

4.1.1. It is an inherent Government function under the "housekeeping" principles authorized by the U.S. Congress for a Government agency to protect its facilities and their occupants from harm and its information and technology from improper disclosure.

4.1.2. HSPD-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," and Federal Information Processing Standards (FIPS) 201, "Personnel Identity Verification (PIV) of Federal Employees and Contractors, " requires appropriate investigation and adjudication for reliability prior to the issuance of permanent NASA photo-ID.

4.1.3. This chapter establishes position risk designation process, security investigative requirements, and reliability determinations for NASA contractors, Intergovernmental Personnel Act (IPA) personnel, grantees, research associates, co-op students, associated foreign nationals, lawful permanent resident(PARs), volunteers, (hereinafter known as contract employees), located on or within a NASA Center, component facility, or accessing NASA information systems remotely.

4.1.4. NASA contractor employees who are granted continuing and official unescorted access to Government facilities, buildings, information, and IT resources are subject to specific investigative requirements similar to the suitability determination requirements imposed by statute upon NASA Federal employees in chapter 3. This investigation provides NASA management necessary information to determine if an individual's fitness or eligibility to promote the efficiency of NASA's mission, initial access or continued presence on the installation, and access to unclassified IT resources is consistent with the safety and security of the U.S. Government, NASA, and the individual Center.

4.1.5. No NASA contractor employee shall be issued a permanent NASA photo-ID, granted access to NASA Centers or facilities, granted access to NASA IT systems, or sensitive information without, at a minimum, the completion of a NAC and submission of required investigative paperwork required to complete the" Inquiries" portion of the NACI, and interim favorable access determination by NASA Security Officials. (The NAC must be accomplished prior to or NLT than 10 working days after start of employment.)

a. Temporary photo ID or visitor badges, issued to contractor employees, who have not submitted the appropriate investigations forms, will expire at the 10 working day time period.

b. Further delays in forms submittal will require the individuals' supervisor to sponsor one-day visit requests up to an additional 5 working days. The supervisor will also be required to escort the individual.

c. Upon expiration of the additional 5 working days, all issued temporary badges/passes and approved accesses will be terminated pending submittal of completed forms. Centers must establish the necessary procedures to ensure abuse of the visitor/temporary badging system does not occur.

4.2 Applicability

4.2.1. This chapter is applicable to NASA contracts, grants, cooperative agreements, and other binding agreements (MOA, MOU, etc.) that meet one or all of the following criteria:

4.2.1.1. For Services (research, operations, support);

4.2.1.2. Performed on or within Government facilities, and/or;

4.2.1.3. Require remote access to unclassified NASA IT Systems.

4.2.2. Unlike many Federal agencies, NASA's user community is a very diverse group which includes U.S. citizens, non-U.S. Citizens (lawful permanent resident (LPR's)) and Foreign Nationals) employed by NASA component facilities, contractor organizations, international partners working under the terms of an intergovernmental agreement, university partners working under a grant, individual personnel volunteering their services, private consultants, or other organizations providing support to NASA via memorandums of agreement (MOA) or memorandums of understanding (MOU).

4.2.3. The requirements of this chapter are designed to be equitable with the employment suitability criteria for NASA Civil Service employees, outlined in chapter 3, and shall be uniformly and consistently applied to ensure maximum protection of NASA assets.

4.2.4. Non-federal employees and contractor personnel of tenant organizations shall maintain Center access eligibility in accordance with this chapter and any Center specific processes and procedures established.

4.3 Responsibilities

4.3.1. The AA/OSPP is responsible for establishing and maintaining a viable and consistent personnel security program in accordance with current personnel security and suitability policies, procedural requirements, and guidelines, as established by the Office of Personnel Management (OPM).

4.3.2. Each Center Director is responsible for ensuring full Center compliance with the provisions set forth in this chapter.

4.3.3. All directors, program managers, line managers, and supervisors, using contractor services as described in paragraph 4.2 above, are responsible for ensuring the successful implementation of this chapter within the area of their authority.

4.3.4. The CCS shall assist, as necessary, in the individual contract and contract position risk designation process and shall establish written procedures for the following:

a. Maintaining and distributing forms, including instructions for the completion of all forms and documentation required for the personnel security reliability investigative process.

b. Assuring the appropriate investigation has been conducted for each NASA contractor employee position.

c. Exercising appropriate risk management authority when investigative results have not been received in a timely fashion (normally within 90 - 120 days) requiring the need to make a decision to deny access, or grant interim or final access, as appropriate.

d. Referring medical related data in investigative files to the appropriate medical authority for review and evaluation, as applicable.

e. Conducting local records checks (LRC) when necessary to clarify, expand, or mitigate information that has been forwarded to the CCS.

f. Making appropriate notifications for:

(1) Confirmation of the results of a favorable access determination.

(2) Actions as a result of a non-favorable access determination.

g. Maintaining, in accordance with the Privacy Act and existing NASA system of records, individual personnel security files on all investigated personnel and reviewing applicable reports with officials in the review process who shall make the determination relative to continued access or revocation of access privileges. Files must contain, at a minimum:

(1) Copies of all investigative results,

(2) Any adverse information reports on affected contractor employees,

(3) Copies of documents pertaining to FN permanent residence or naturalization status.

4.3.5. The NASA General Counsel or the Chief Counsel of each Center, as appropriate, shall provide legal counsel with regard to implementation of this chapter.

4.3.6. Contract Management Officials (e.g., Contractor Management, COTR, Project Managers) shall ensure full compliance with this chapter.

4.4 Designation of Security Risk Levels

4.4.1. All contracts, grants, cooperative agreements, or other binding agreements (MOA or MOU) that meet the criteria in section 4.2 above, shall be categorized by security risk level. Each document shall include a security risk level designation of one of the following:

- High Risk;
- Moderate Risk; or
- Low Risk

4.4.2. The contract security risk level designations shall be made by the NASA Center program office representative (typically the designated Civil Service project manager (sponsor) or COTR), in coordination with the CCS, appropriate IT Security Manager(s), and contractor HR Offices. The parties shall review the work to be performed and, following the process flow established in Appendix N " Determining Position Risk and Sensitivity Levels, Process Flow Chart" and assign the highest security risk designation in accordance with the criteria established in Appendix M, "Designation of Public Trust Positions and Investigative Requirements."

4.4.3. The security risk level is determined by evaluating the sensitivity and risk of the work being performed and accesses required by the contractor and the potential for damage to NASA's mission and operations if performed inefficiently, ineffectively, or in an unsafe or unethical manner. Included in this is the requirement to properly identify and assign risk

level designations for those individual positions directly involved in IT systems and/or application software development commensurate with the risk level that will ultimately be applied to the system and/or application when deployed. Section 4.6.2 and 4.6.5.1 is applicable.

4.4.4. The risk level, in turn, determines the investigative requirements for the contractor personnel who shall perform the work.

4.4.5. The sponsoring program or project office shall ensure the contractor meets the requirements of this chapter.

4.5 NASA Contractor Employee Position Risk/Sensitivity Level Criteria and Designation Process

4.5.1. Security risk levels for contracts, grants, cooperative agreements, and MOA or MOU shall be established by program or project management and contractor management who, in coordination with the CCS, the IT System Line Manager, and IT System Security Administrator, shall review the work to be performed under the contract or grant and assign to the entire contract, grant, cooperative agreement, MOA, or MOU the highest security risk designation in accordance with the criteria established in this section.

4.5.2. Accordingly, each individual NASA contractor employee shall undergo security screening processing according to the contract, grant, MOA, MOU, and individual position risk designation levels as determined using the criteria in this section and the process flow established in Appendix N " Determining Position Risk and Sensitivity Levels, Process Flow Chart" and Appendix M, this NPR.

4.5.3. In instances where there is a wide variance in the security risk level of the work to be performed under a contract, grant, MOA, MOU, or other binding agreement, individual contractor employees must be processed at the risk designation commensurate with their duties. In meeting this contingency, the contract, grant, MOA, or MOU must specifically apply controls to ensure that work of the lower risk positions does not overlap with that for the higher risk positions.

4.5.4. The contractor shall identify the employees to be processed at each risk designation and shall specify the duties of the positions. An example of such a case is custodial work, where some NASA contractor employees may work unmonitored during working hours, in a building which houses classified information, or in a facility designated as Mission Essential Infrastructure (MEI) or other security area designation that requires a higher degree of trust.

4.5.4.1. The entire contract, grant, MOA, or MOU may be designated High or Moderate Risk due to the former case, but those NASA contractor employees whose work would be Moderate or Low Risk must be investigated accordingly.

4.5.4.2. The contractor and COTR must specify control measures to be used to ensure that there is no overlap of work duties between the lower designated positions.

4.5.5. All access factors (i.e., Center, facility, information, and IT systems) must be considered concurrently, as part of the overall risk designation process. This procedure serves to avoid duplication of effort by eliminating the possibility that a single individual could be assessed numerous times for different accesses. The intended result will be that the highest risk level designation (e.g., IT-6C = High Risk designated position compared against that same individual's need to access uncontrolled areas of the Center = Low Risk) is the designation for which the appropriate investigation will be conducted.

4.5.6. Position risk level determinations are inclusive of many factors. Generally, they are represented in the categories below:

a. **High Risk** positions involve duties that are especially critical to the Agency and its programs and operations, with a broad scope of policy or program authority such as policy development and implementation; higher level management assignments; and/or non-management positions with authority for independent action. High Risk positions may

also include national security positions as described Chapter 6.

b. **Moderate Risk** positions involve duties of considerable importance to the Agency and its programs and operations with significant program and/or operational responsibilities such as: assistants for policy development and implementation; mid-level management assignments; non-management positions with authority for independent or semi-independent action; or positions that demand public confidence or trust. Moderate Risk positions may also include national security positions as described in Chapter 6.

c. **Low Risk** positions involve duties with limited relations to the Agency and its programs and operations and which have little affect on the efficiency of the Agency's programs and operations. Low Risk positions may also include national security positions as described in Chapter 6.

d. Provided below are categories of positions and/or specific duties that are unique to NASA and therefore, may influence the risk level designation for each individual position.

(1). Information Technology (IT) Resources Positions.

(a). In accordance with the Federal Information Systems Management Act (FISMA), the Office of Management and Budget (OMB) Circular A-130, and NPR 2810.1, NASA has established personnel security requirements and procedures to assure an adequate level of protection for NASA IT systems, which includes the appropriate screening of all individuals having access to NASA IT systems.

(b). The level of reliability checks or investigations range from a NACI to a full-field background investigation, depending upon the sensitivity of the information to be handled and the risk and magnitude of loss or harm that could be caused by the individual.

(1) **High Risk or 6C** positions include positions in which the incumbent is responsible for planning, directing, and implementing a computer security program; has major responsibility for directing, planning, and designing an IT system, including development activity associated with hardware and software; or, can access a system with relatively high risk for causing grave damage or realizing a significant personal gain. High Risk IT positions may include positions that involve:

(a) Developing or administration of Agency IT Security Programs, directing or controlling IT risk analysis and threat assessments, or conducting investigations.

(b) Significant involvement in life-critical or mission-critical systems (see paragraph 4.6.;

(c) Privileged access to Mission Essential IT Systems (See section 4.7. for further requirements).

(d) Access to data or systems whose misuse can cause very serious adverse impact or result in significant personal gain.

(e) Assignments involving accounting, disbursement, or authorization of $10 million dollars or more per year.

(f) Privileged access to IT systems whose misuse can cause "significant adverse impact" to NASA missions. These systems include those that interconnect with a NASA network in such a way as to enable the user to bypass firewalls or systems operated by a NASA contractor whose function and data has substantial value, even if these systems are not interconnected to a NASA network. (NOTE: Foreign Nationals (FN) are not authorized to have "Privileged" access to NASA IT Systems. The only exception is an FN who is involved in an international program or project under an International Space Act Agreement (ISAA). IT System Line Managers contemplating the granting of such access shall consult with their Center Export Administrator and Center International Visit Coordinator (IVC) to ensure that an ISAA is in place, that the ISAA includes such a requirement, and that the international program or project involved certifies the need for such access.)

(2) **Moderate Risk or 5C** positions include positions where the incumbent is responsible

for directing, planning, designing, operating, or maintaining IT systems and whose work is technically reviewed by a higher authority (at the high risk level) to insure the integrity of the system: Moderate risk IT positions may involve:

(a) Systems design, operation, testing, maintenance, or monitoring which is under technical review of IT-1 and includes:

(1) Those that contain the primary copy of data whose cost to replace exceeds $1 million.

(2) Those that control systems which affect personal safety and/or physical security, fire, or Hazmat warning safety systems.

(3) Privileged information on contract awards in excess of $10 million.

(4) Accounting disbursement or authorization of more than $1 million, but less than $10 million per year.

(b) Access to data or systems whose misuse can cause serious adverse impact or result in personal gain.

(1) Proprietary data:

(2) Privacy Act protected information:

(3) Export Control Regulations (EAR), International Traffic in Arms Regulations (ITAR), and the Militarily Critical Technologies List (MCTL) information.

(c) "Limited privileged" access to IT systems whose misuse can cause "adverse impact" to NASA missions. [NOTE: Foreign Nationals (FN) are not authorized to have "Limited Privileged" access to NASA IT Systems. The only exception is an FN who is involved in an international program or project under an ISAA. IT System Line Managers, contemplating the granting of such access shall consult with their Center Export Administrator and Center International Visit Coordinator (IVC) to ensure that an ISAA is in place, and that the ISAA includes such a requirement, and that the international program or project involved certifies the need for such access.]

(3) **Low Risk or 1C** positions are all IT system positions that do not fall in the categories above and includes all non-sensitive positions and all other positions involving IT Systems whose misuse has limited potential for adverse impact or sensitive data is protected with password and encryption. Low risk IT positions may involve:

(a) General word processing;

(b) Systems containing no IT-I or IT-II level information or IT-1 or IT-2 level information that is protected from unauthorized access.

(c) Positions that provide for no privileged or limited privileged access or do not afford IT-1 or IT-2 access. Includes: Systems that contain Sensitive But Unclassified (SBU) as described in chapter 5, section 5.24. These requirements do not apply to NASA web-pages established for general public access. These web-pages are prohibited from containing classified information or NASA Sensitive But Unclassified (SBU), or providing unprotected links to NASA "Private" domains.

(4) Specific requirements and criteria for designating Computer/ADP risk levels are contained in Appendix M.

(2) CHILDCARE WORKER EMPLOYEE RELIABILITY INVESTIGATIONS (42 U.S.C. 13041) - Reliability investigations are to be completed on all childcare providers prior to working in NASA-sponsored childcare facilities.

(a) Personnel shall work under regular and continuous observation by a favorably investigated employee pending completion of the investigation.

(b) NASA childcare centers shall coordinate **all** personnel hiring actions with the Center Security Office prior to entry on duty. NASA childcare center management may NOT override these requirements.

(c) Per OPM Federal Investigations Notice #98-06, Subject: "Child Care Provider Investigations," Centers shall use the services of OPM to conduct these investigations.

4.5.7. When a NASA contractor employee's duties require any overlap into a higher or lower risk level, the position sensitivity designation must then be set at the highest risk level anticipated.

4.5.8. Personnel investigated and favorably adjudicated within the previous 3 to 5 years under the provisions of Chapter 6 of this NPR may be considered fully qualified to occupy any position established under this chapter.

4.6 Contractor Coordinated Background Investigations for U.S. Citizen Employees

4.6.1. With the exception of the NASA Child Care Center program, obtaining background investigations for each contractor employee (U.S. Citizen only) at the **Low** and **Moderate Risk** Levels are to be the responsibility of the contractor at some time in the near future when the Federal Acquisition Regulations (FAR) are updated to reflect this new mandate. Therefore, this section will apply only after the FAR is updated and implemented.

a. Pending update and implementation of the FAR, section 4.7. is applicable.

b. Investigations may only be conducted by the Office of Personnel (OPM) or Defense Security Service (DSS) at the request of the contractor. The investigations conducted by OPM or DSS follow the requirements of all pertinent Federal statutes, regulations, executive order, and presidential directives and fully meet the requirements of this chapter. Refer to Chapter 10 for definitions of the various types of investigations required. Results of investigations will be made available to the CCS through the DSS.

4.6.2. NASA shall conduct the appropriate security screening for all foreign national contractor employees regardless of the position risk level designation and access requirements.

4.6.3. Position Risk Designation Management for Non-U.S. Citizens (Foreign Nationals and Permanent Resident Aliens) **(See Section 4.10 for overall guidance on Foreign National contractor employee security screening.)**

a. Non-U.S. citizens (including lawful permanent residents (LPR)) are eligible for placement in **Low** and **Moderate** risk positions, but are not normally eligible for employment in positions designated as **High Risk** . Under specific situations the AA/OSPP may authorize the placement of a non-U.S. citizen for a specific **High Risk** position when it has been determined that no U.S. citizen has the skills necessary to perform the work. The requesting organization shall submit a written request to the AA/OSPP via the CCS. The request shall:

(1) Specify why it is impractical or unreasonable to use U.S. Citizens to perform the required work or function.

(2) Define the individual's special expertise.

(3) Define the compelling reasons for the request.

b. The CCS shall review the request for accuracy, endorse or non-endorse it, and forward it to the AA/OSPP.

c. The AA/OSPP shall coordinate with the Office of External Affairs for concurrence (Export Compliance), and if approved, shall return it to the requestor. A copy shall be retained in the OSPP and CCS files.

4.6.3.1. A completed background investigation and favorable adjudication are required before the position may be occupied and access granted. Foreign National personnel must:

a. Be entered into the NASA Foreign National Management System (FNMS) by the sponsoring organization and processed by the Center International Visits Coordinator (IVC) to ensure they:

b. Have legal visa status with the U.S. Citizenship and Immigration Services (USCIS) and U.S.-VISIT Program.

c. Have advance sponsorship and concurrence from Program Management, Center International Visits Coordinator (IVC), CCS, Center Export Administrator (CEA), appropriate System Administrator, and IT Security Manager(s).

d. Undergo a review of Central Intelligence Agency (CIA), U.S. Department of State, and Bureau of Immigration and Customs Enforcement (BICE) databases as necessary and available.

4.6.3.2. Denied requests shall be returned to the requestor with an explanation of the denial.

4.6.4. The AA for Security and Program Protection may waive some, or all, investigative requirements for representatives of foreign Governments who request, in writing, access to NASA IT systems pursuant to an intergovernmental agreement. Access shall be limited to that which is necessary to execute the agreement.

4.6.4.1. Foreign national personnel with approved placement in **High Risk** positions shall be closely monitored. All personnel shall be made aware of access limits imposed on these individuals and shall ensure compliance with any restrictions imposed.

4.6.4.2. Any requests for FN access to sensitive information owned by another agency must be coordinated with and approved by that agency.

4.6.5. Subsequent reinvestigative requirements established in section 4.16 remain in effect.

4.7 Contractor Personnel Security Background Investigations Conducted by NASA

4.7.1. Per FIPS 201 NASA is responsible for ensuring appropriate investigations are conducted and access suitability determined for all contractor personnel.

a. When the contractor has not accomplished the required background investigations the Center CCS must ensure the appropriate investigation is conducted, in the following manner:

(1). The sponsoring NASA program shall provide NASA security offices with necessary funding to accomplish the required investigations.

(2). The COTR shall notify the CCS who shall make the necessary blank investigative forms, identified in section 4.8, available to the contractor. Forms shall be made available using the web-based e-QIP system).

4.7.2. The NASA contractor employee shall complete and submit the forms, with appropriate written releases of the Government from liability, to the CCS through the use of electronic web-based investigative forms as stated in paragraph 4.8.

4.7.3. The timing of security form submittal and the established risk level may dictate whether a proposed NASA contractor employee can begin work prior to a final access determination. Based on the specifics of the situation and a preliminary review of the submitted forms, the CCS shall advise the COTR whether the individual can commence working prior to the receipt of the completed investigation and final access determination.

4.7.4. Pre-assignment Checks for **High Risk** Positions.

4.7.4.1. Upon selection, but prior to assignment, the Contracting or Grants Officer shall direct the NASA contract employee or company to complete the required security

investigative forms for the High Risk position (refer to section 4.8) and return them to the CCS for review and investigative action.

.7.4.2. Upon review of information in the completed forms, the CCS may:

a. Interview the prospective NASA contractor employee to resolve any issues; or,

b. Request investigation through NASA channels and await final results; or,

c. Conduct further screening, as appropriate to resolve any issues; or,

d. Grant interim authority to access a NASA Center pending receipt of completed investigation and final access approval determination; or,

e. Deny access and take the necessary actions per section 4.11.

4.8 Forms Required to Request an Investigation

ACTION	LOW RISK POSITION	MODERATE RISK POSITION	HIGH RISK POSITION
NON-NASA PERSONNEL	NACI/No Access SF 85 - e-QIP OFI Form 79B, FC 258	NACI/No Access SF 85P - e-QIP FC 258, OFI Form 79B, NASA Form 1684 (Authorization and Release of Credit Reports)	BI SF 85P - e-QIP FC 258, OFI Form 79B, NASA Form 1684 (Authorization and Release of Credit Reports)

4.9 Adjudication Process for Access

4.9.1. When the results of the completed personnel security investigation has been made available, the CCS shall determine if the individual is eligible for the type of accesses required for the work.

4.9.1.1. In cases that contain significant adverse information, the personnel security investigation is not complete until a subject interview described in section 4.11.3 has been conducted.

4.9.1.2. The CCS, or designee, shall make the final determination based on the results of the DSS investigation

4.9.2. All personnel involved in the adjudication process shall be trained in adjudication methods and shall keep their training current. NASA shall follow established OPM suitability adjudicative guidelines in order to determine a contractor's suitability status. The process shall examine the facts in the investigation and result in a determination that an individual is or is not eligible for access, or continued access, to NASA facilities, information, or IT systems.

4.9.3. When adverse information becomes known about a NASA contractor employee who already has access to NASA facilities or IT systems and the initial Entry on Duty (EOD) required personnel security reliability investigation has been completed and favorability adjudicated, the adjudicator shall consider whether the individual:

- Voluntarily reported the information;
- Was cooperative, truthful, and complete during the investigation;
- Sought assistance and followed professional guidance;

- Resolved or appears likely to favorably resolve the concern;
- Has demonstrated positive changes in behavior and employment.

4.9.4. The CCS may approve conditional access based on mitigating factors. The CCS may also require written agreements with the NASA contractor employee certifying that any future adverse actions would be grounds for immediate revocation of access.

4.9.5. If the CCS decides to deny or revoke access, the CCS shall notify the individual, formally and in writing, of NASA's decision and include the reasons that were used to make the determination. The individual shall also be informed of the provisions of the Privacy Act and the Freedom of Information Act and how to obtain official copies of any pertinent investigation.

4.9.6. If a final decision to deny or revoke access is made, the CCS shall notify the contractor through the COTR and the CO that the individual is not eligible for the needed access.

4.9.6.1. The CO shall inform the NASA contractor of NASA's decision and provide a statement that NASA's decision is not intended to imply that the individual's employment elsewhere in the company should be affected.

4.9.6.2. Adverse information shall not be disclosed to the individual's employer since it could affect the individual's employment and possibly subject NASA to legal liability.

4.9.7. NASA Security Offices, in consultation with responsible program officials and IT Security Managers, may grant interim access to NASA facilities and IT systems, if the submitted forms do not contain adverse or questionable information.

4.9.8. NASA reserves the right to immediately and unilaterally revoke or suspend such interim access in the event that adverse information is developed.

4.10 Escort Requirements in Lieu of Completed Favorable Background Investigations

4.10.1. While the most desirable procedure for the utmost safety and security of NASA personnel and facilities would be total escort of non-affiliated personnel (visitors, unscreened contractors, delivery personnel, Foreign Nationals, U.S. Representatives of Foreign entities, etc.), this NPR recognizes the limitations and potential cost associated with such a policy.

4.10.2. U.S. Citizens: Each Center shall develop and implement procedures for the proper escort of non-affiliated U.S. citizen visitors and NASA contractor employees when the completion and receipt of an appropriate personnel security reliability investigation is not readily available and the visit is under 30 days or is intermittent that would warrant the submission of, at a minimum, a NAC investigation. Decisions not to escort shall be made by the CCS, supported by appropriate consideration of the risk involved, the areas and information to be accessed, availability of certification by the individual's employer that the appropriate reliability investigation has been conducted, and the implementation of compensatory security measures, as appropriate, to prohibit unauthorized access.

4.10.3. Foreign Nationals (FN): FN visitors, representatives, or contractor employees (including permanent resident aliens) requiring access to a NASA Center for a period exceeding 30 days shall be managed in accordance with the following requirements:

a. Due to the strict investigative requirements for positions designated at the High Risk level, foreign nationals will not normally be eligible to assume duties designated at High Risk. Sponsors desiring to place a foreign national in a high risk position must follow the procedures established in section 4.6.3 of this NPR.

b. All foreign nationals from designated and non-designated countries shall be escorted at all times pending the completion of the requisite personnel security reliability investigation and favorable determination.

c. Upon a favorable determination, individual compensatory security measures (e.g., information/data access, on-Center movement restrictions) in the form of a written agreement titled, "Security/Technology Control Plan," shall be developed, agreed upon, and signed by the individual FN visitor, visit sponsor, Center Export Administrator, International Visits Coordinator, and CCS.

(1) FN visitors, representatives, or FN contractor employees (including PRA's) from a non-designated country shall not be granted unescorted access privileges to NASA Centers after normal working hours unless specifically justified and included in the Security/Technology Control Plan. See Appendix K for a Security/Technology Control Plan Template.

(2) FN visitors, representatives, or FN contractor employees (to include PRA's) from designated countries shall not be granted unescorted access privileges to NASA Centers after normal working hours unless the employee can be effectively monitored and appropriate controls implemented that establishes strict accountability during the access period. Establishment of movement and access controls must be document in a Security/Technology Control Plan. See Appendix K for a Security/Technology Control Plan Template.

(3) Compliance with the FN access plan must be validated by the Center security office through periodic random visits by security personnel.

(4) Violations of established FN visit protocols will be properly investigated by Center CI agents, and action taken, including termination of visit or access, when warranted. All violations of FN visit protocols will be reported to the Director, Safeguards Division.

(5) Security/Technology Control Plans shall be reviewed for continued applicability upon changes in visitor status (e.g., visit extension/renewal, new project parameters, etc.).

4.10.4. Foreign National visitors, representatives, or contractor employees who are visiting 30 days or less, and for which the cost and time of conducting a satisfactory security reliability check may not be warranted, shall be escorted at all times unless a previous satisfactory investigation has been conducted within the last 3 years. Escorts must be permanently NASA photo-ID'd Civil Service employee or Contractor Employees possessing U.S. Citizenship.

4.10.5. Foreign national visitors of less than 30 days, working under an implemented International Space Act Agreement (ISAA) as defined in NPD 1050.1G, "Authority to Enter Into Space Act Agreements," NPD 1360.2A, "Initiation and Development of International Cooperation in Space and Aeronautics Programs," and NPR 1050.1, "Space Act Agreements," must be escorted by a permanently assigned NASA photo-ID'd U.S. citizen or a NASA permanently assigned NASA photo-ID'd foreign national currently working under an ISAA (e.g., FN Astronauts, ISS, etc.) . E scorts by a Foreign National or U.S. person (LPR) under this paragraph is permitted only in those areas authorized by the ISAA .

4.11 Adverse Information

4.11.1. When adverse information is developed or received in the course of any personnel security investigation or subsequent to such investigation and initial favorable determination, the scope of inquiry shall be expanded to the extent necessary to obtain sufficient information to make a determination that the contractor shall or shall not be (or continue to be) granted access to NASA facilities or IT systems.

4.11.1.1. These expanded inquiries may be conducted by a NASA security official with appropriate investigative experience, NASA contracted investigators, by the original investigating agency, or by an agency of the Federal Government at NASA's request.

4.11.1.2. Investigative expansion may consist of many different lines of inquiry, including but not limited to, interviews of the subject, supervisors, co-workers, neighbors, physicians, records checks with various local agencies, and credit checks.

4.11.1.3. Releases from the subject shall be obtained when required to pursue additional leads (e.g., medical records and credit checks).

4.11.2. Counterintelligence-related adverse information is to be relayed as soon as possible, but no later than the next business day after the information has been obtained, to the Center counterintelligence office or the NASA Office of Security and Program Protection.

4.11.3. A NASA contractor employee on whom significant unfavorable or derogatory information has been developed or received during the personnel security reliability process must be confronted with the information and offered an opportunity to refute, explain, clarify, or mitigate the information in question prior to final access determination.

4.12 Tenant Organization Employee and Contractor Reliability

4.12.1. NASA Centers hosting tenant organizations necessitating access to tenant facilities located in Center controlled areas shall establish appropriate processes and procedures to ensure full compliance with this chapter.

4.12.2. Approval for accessing tenant facilities does not constitute authority for accessing NASA facilities unless authorized by local center policy.

4.13 Reinvestigation Requirements

4.13.1. At a minimum, reinvestigations conducted under this chapter shall be conducted every 5 to 7 years, or sooner for cause, for all High and Moderate Risk contractor, grantee, MOA, or MOU positions to ensure maintenance of eligibility under the Continuous Evaluation Program (CEP) for access to NASA Centers , facilities, and information.

4.13.2. Positions at the Low Risk Level are be subject to reinvestigation every 10 years, at any time for cause, or at the discretion of the individual Center.

4.13.3. Re-investigations shall also be conducted upon position assignment change when the change involves moving to a higher risk level position.

4.13.4. All reinvestigations, except those conducted as a result of moving to a higher risk level position, will be comprised of a National Agency Check with Inquiries (NACI), local records check, as necessary, and personal interview by a qualified investigator, as necessary.

4.14 Recordkeeping

Records and information related to this chapter shall be managed per procedures established in chapter 2, section 2.18 of this NPR.

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | AppendixJ | AppendixK | AppendixL | AppendixM | AppendixN | AppendixO | ALL |

| NODIS Library | Organization and Administration(1000s) | Search |

DISTRIBUTION:
NODIS